Amendments to the Specification

Please replace the paragraph beginning on page 3, line 20, with the following rewritten paragraph:

~~Ones~~ Information obtained by cutting out the access control matrix for every column ~~correspond~~ corresponds to information descriptive of operation privilege allowed for respective subjects or users by objects, which is called "Access Control List: ACL". In the example shown in "Table 1", for example, the column corresponding to "File#1" is an access control list indicative of operation privilege given to Alex, Bob and Cod for the ~~objects~~ objects, respectively. ~~"Unix"~~ "Unix", widely used as an operation system (OS) for a server or development ~~platform~~ platform, makes use of a simplified access control list.

Please replace the paragraph beginning on page 3, line 27, with the following rewritten paragraph:

Further, ones obtained by cutting out the access control matrix for every row correspond to information descriptive of operation privilege allowed for respective objects by subjects, i.e., users, which is called "privilege information" or "capability (Capability)". For example, a first row of the access control matrix shown in "Table 1" corresponds to the capability related to the user "Alex". Further, a second row corresponds to the capability related to the user ~~"Box".~~ "Bob".

Please replace the paragraph beginning on page 5, line 13, with the following rewritten paragraph:

However, according to the method disclosed in Japanese Published Unexamined Patent Application No. Hei 5-81204, it cannot cope with variations in capability such as an expiration date of use and the number of accesses. Further, ~~it no refers to a~~ no method of freely creating a PAC weakened in capability by the starter ~~subject.~~ subject is disclosed.

Please replace the paragraph beginning on page 5, line 22, with the following rewritten paragraph:

However, the invention according to Japanese Published Unexamined Patent Application No. Hei 9-319659 is not one applied to a distributed environment under which the capability cannot be protected in safety. Further, the same publication ~~no refers to a~~ refers to no method of safely inspecting capabilities between objects.

Please replace the paragraph beginning on page 7, line 23, with the following rewritten paragraph:

A paper of Bjorn N. Freeman-Benson open to the public on a Web, "Using the Web to Private Information –or- A Short Paper About Password Protection Without Client Modification" ~~(URL: "hyperlink "http://www1.cern.ch/www94/PrelimProcs.Html")~~ discloses the handling of a confidential URL (i.e., capability). A method described in the same paper follows a procedure shown below.

Please replace the paragraph beginning on page 8, line 19, with the following rewritten paragraph:

~~It~~ If the above is summed up, then the prior art has the following problems:

(1) It is difficult to safely manage and transfer capabilities in association with variations diversified in privilege contents such as the expiration date of usage and the number of valid uses.

Please replace the paragraph beginning on page 19, line 2, with the following rewritten paragraph:

First, each client for transferring privilege information generates privilege information weakened in its own privilege contents. Further, the client applies a calculating operation such as a one-way function to a bit string obtained by concatenating the generated privilege information and private or secret information, thereby generating first protected privilege

information having eliminated the danger of its bad use. Thus, ~~none of~~ no third parties who do not know the private information ~~is~~ are able to freely tamper with the first protected privilege information.

Please replace the paragraph beginning on page 20, line 13, with the following rewritten paragraph:

Further, the access privilege transferring method according to the third aspect of the present invention is one wherein an encryption function is used as a predetermined calculating operation for protecting privilege information to be transferred, without using a one-way function. Secret or private information shared between each client and a server can be used as an encryption key for the encryption function. Both of a symmetric private key cryptosystem ~~/*/ and~~ and a public key cryptosystem can be applied as a cryptosystem. The symmetric private key cryptosystem is a system wherein the same private key is shared between communication partners or objects and capable of decrypting encrypted information by using the same key as the private key used for encryption. In contrast to it, the public key cryptosystem is a system wherein information is encrypted and decrypted by a combination of two keys having such properties that information encrypted by one key can be decrypted by the other key alone. It is common that one key is held by a user individual as a "private key" held in secrecy and the other key is used as a "public key" open to the public for the third parties. Encrypting information with the public key, for example, makes it possible to safely transmit a secret or private document to a private-key's owner. Owing to the transmission of a signature encrypted using the private key, a receiver can authenticate the signature through the use of the public key.

Please cancel the heading "<<Notes>>" on page 23.

Please cancel the paragraph at page 23, lines 12-22.

Please replace the paragraph beginning on page 26, line 22, with the following rewritten paragraph:

Fig. 1 typically shows a distributed computing environment according to the first embodiment of the present invention. The first embodiment is one for applying a one-way function MD (Message Digest) to privilege information to thereby implement safe transfer of an access privilege or right. Respective parts will be described below.

Please replace the paragraph beginning on page 27, line 6, with the following rewritten paragraph:

In the example shown in Fig. 1, the HTTP server 300 will be represented by a URL given as "hyperlink ~~"http://www300".~~ http://www300". Further, the HTTP server 300 has an access control object 301, and N HTTP objects designated at reference numerals 391 through 39N. The respective HTTP objects 391 through 39N will be indicated by URLs given as "hyperlink ~~"http://www300/object391", ..., "http://www300/object39N",~~ http://www300/object391, ..., http://www300/object39N", respectively. Further, the access control object 301 is an object for controlling an access request to each of the HTTP objects 391 through 39N. However, the access control object 301 does not necessarily require the existence thereof over the same server as that for the HTTP objects 391 through 39N. The access control object 301 exists over another host (not shown), for example and may be invoked or called up from the HTTP server 300 on a remote basis so as to start up a predetermined access control process.

Please replace the paragraph beginning on page 29, line 9, with the following rewritten paragraph:

Next the client 100 bit-concatenates the password1 used as the ~~secrete~~ secret information with the privilege information capability1 from behind the character string and

applies the one-way function MD ~~(Message Digest)~~ thereto, thereby generating protected right or privilege information capabilityMD1 shown below.

Please replace the paragraph beginning on page 29, line 16, with the following rewritten paragraph:

The one-way function MD is a function so difficult to determine its inverse function and has the feature of making it impossible to estimate the value of an argument preceding the application of the function MD thereto. Thus, third parties who do not know the ~~secrete~~ secret information password1 are not able to freely tamper with the protected privilege information capabilityMD1.

Please replace the paragraph beginning on page 29, line 26, with the following rewritten paragraph:

As already described above, the third parties (including the client 200) who do not know the ~~secrete~~ secret information password1, are not able to tamper with the protected privilege information capabilityMD1. It is thus understood that the client 100 is able to safely transfer access rights or privileges to the HTTP object 391 to another client 200.

Please replace the paragraph beginning on page 32, line 10, with the following rewritten paragraph:

~~Let's assume~~ Assume that as a premise of the transactions, the client 100 holds therein its user information "userid1" and password "password1" as an account (qualifications for a user) for an access to the HTTP server 300. Further, the access control object 301 of the HTTP server 300 stores therein the combinations (userid1, password1), (userid2, password2), ... of the user information about the respective clients 100 ... and their passwords as the "password management table".

Please replace the paragraph beginning on page 32, line 18, with the following rewritten paragraph:

Next, the client 100 applies the one-way function MD to a bit string obtained by bit-concatenating its own ~~secrete~~ secret information password1 with the rear of the privilege information capability1 to thereby generate protected privilege information capabilityMD1 (Tr2).

Please replace the paragraph beginning on page 35, line 13, with the following rewritten paragraph:

Next, the client 100 bit-concatenates the password1 used as the ~~secrete~~ secret information with the privilege information capability1 from behind the character string and applies a one-way function MD ~~(Message Digest)~~ thereto, thereby generating protected privilege information capabilityMD1 shown below.

Please replace the paragraph beginning on page 35, line 20, with the following rewritten paragraph:

The one-way function MD is a function so difficult to determine its inverse function and has the feature of making it impossible to estimate the value of an argument preceding the application of the function MD thereto. Thus, third parties who do not know the ~~secrete~~ secret information password1, are not able to freely tamper with the protected privilege information ~~capbilityMD1.~~ capabilityMD1.

Please replace the paragraph beginning on page 36, line 3, with the following rewritten paragraph:

As already described above, the third parties (including the client 200) who do not know the ~~secrete~~ secret information password1 are not able to tamper with the protected privilege information capabilityMD1. It is thus understood that the client 100 is able to safely transfer access privileges to the HTTP object 391 to another client 200.

Please replace the paragraph beginning on page 39, line 15, with the following rewritten paragraph:

~~Let's assume~~ Assume that as a premise of the transactions, the client 100 holds therein its user information "userid1" and password "password1" as an account (qualifications for a user) for an access to the HTTP server 300. Further, the access control object 301 of the HTTP server 300 stores therein the combinations (userid1, password1), (userid2, password2), ... of the user information about the respective clients 100 ... and their passwords as the "password management table".

Please replace the paragraph beginning on page 39, line 23, with the following rewritten paragraph:

Next, the client 100 applies the one-way function MD to a bit string obtained by bit-concatenating its own ~~secrete~~ secret information password1 with the back of the privilege information capability1 to thereby generate protected privilege information capabilityMD1 (Tr12).

Please replace the paragraph beginning on page 43, line 9, with the following rewritten paragraph:

Next, the client 100 encrypts the privilege information capability1 by using its own ~~secrete~~ secret information password1 to thereby generate protected privilege information capabilityCR1 shown below.

Please replace the paragraph beginning on page 44, line 8, with the following rewritten paragraph:

As already described above, the third parties (including the client 200) who do not know the ~~secrete~~ secret or cryptic information password1 are not able to tamper with the protected privilege information capabilityCR1. It is thus understood that the client 100 is able to safely transfer access privileges to the HTTP object 391 to another client 200.

Please replace the paragraph beginning on page 47, line 15, with the following rewritten paragraph:

In the present embodiment, an HTTP server 300 will be represented by a URL given as "hyperlink http://www300". Further, the HTTP server 300 has an access control object 301 and N HTTP objects designated at reference numerals 391 through 39N. The HTTP objects 391 through 39N will be respectively represented by URLs given as "hyperlink ~~"http://www300/object391", ..., "http://www300/object39N".~~ http://www300/object391, ..., http://www300/object39N".

Please replace the paragraph beginning on page 49, line 17, with the following rewritten paragraph:

Next, the client 100 encrypts the privilege information capability1 by using its own ~~secrete~~ secret information password1 to thereby generate protected privilege information capabilityCR1 shown below.

Please replace the paragraph beginning on page 50, line 7, with the following rewritten paragraph:

As already described above, the third parties (including the client 200) who do not know the ~~secrete~~ secret information password1 are not able to tamper with the protected privilege information capabilityCR1. It is thus understood that the client 100 is able to safely transfer access rights or privileges to the HTTP object 391 to another client 200.

Please replace the Abstract with the attached substitute Abstract.